



A damage assessment framework for insider threats to national security information: Edward Snowden and the Cambridge Five in comparative historical perspective

David V. Gioe & Joseph M. Hatfield

To cite this article: David V. Gioe & Joseph M. Hatfield (2020): A damage assessment framework for insider threats to national security information: Edward Snowden and the Cambridge Five in comparative historical perspective, Cambridge Review of International Affairs, DOI: [10.1080/09557571.2020.1853053](https://doi.org/10.1080/09557571.2020.1853053)

To link to this article: <https://doi.org/10.1080/09557571.2020.1853053>



Published online: 07 Dec 2020.



Submit your article to this journal [↗](#)



Article views: 29



View related articles [↗](#)



View Crossmark data [↗](#)



A damage assessment framework for insider threats to national security information: Edward Snowden and the Cambridge Five in comparative historical perspective

David V. Gioe  and Joseph M. Hatfield
US Military Academy

Abstract *A new ‘digital generation’ of insider threat has emerged within the US intelligence community. Edward Snowden’s mass leaks were not the first transparency-driven digital challenge to the United States Intelligence Community (USIC). Three years before, then U.S. Army Private Bradley Manning provided 500,000 classified documents to WikiLeaks, which published them to great fanfare for transparency advocates while causing much concern in Washington. These are not isolated cases; the tempo of such mass public disclosures seems to be increasing. In what ways is this new breed of insider threat akin to more traditional counterintelligence breaches such as those of the Cold War? One central point of comparison is the relative damage caused by each, since it would be difficult to sustain the thesis that a new type of insidious threat has emerged if the damage caused by mass leaks was of little consequence when compared to traditional espionage cases. And ‘damage’ must be evaluated within the social history of the breaches themselves. A systematic approach to the comparison of breaches has remained elusive. This article offers such a framework using the Snowden leak as a case study in contemporary self-tasked digital breaches and the Cambridge Five spy ring as a case study in traditional externally-tasked breaches.*

Introduction

Much ink has been spilled over whether former National Security Agency (NSA) contractor Edward Snowden and those who have followed his example represent a ‘post-modern breed of whistleblower’ (Bamford 2014) or should rather be understood as the latest counterintelligence breach along the lines of traditional penetrations of the Anglo-American intelligence community that occur from time to time.

Snowden’s mass leaks were not the first purely transparency-driven digital challenge to counterintelligence protocols from deep within the American intelligence machinery. Three years before, then U.S. Army Private Bradley (now Chelsea) Manning exfiltrated an unprecedented 500,000 classified documents and provided them to self-described whistleblowing organization WikiLeaks, which published them to great fanfare for transparency advocates while causing much concern in Washington over diplomatic repercussions (Zetter 2010). These are not isolated cases; if anything, the tempo of such mass public disclosures seems to be increasing, adding new intelligence agencies as victims with each new revelation by formerly trusted insiders.

In March 2017, the Central Intelligence Agency (CIA) fell victim to what is known as the ‘Vault 7’ series, in which sensitive computer tools for digital surveillance and cyber operations were given to WikiLeaks and published online, according to press accounts. The following year former CIA software engineer Joshua Schulte was accused of the breach (Goldman 2018). Although Manning, Snowden, and Schulte represent the most significant mass leakers of classified information, others have played smaller roles. For instance, the improbably named NSA contractor Reality Winner printed a sensitive document from an NSA computer system and sent it to the self-described publisher of ‘adversarial journalism,’ *The Intercept*, run by journalist-activists originally linked to the Snowden leaks (Philipps 2018).

What this millennial quartet has in common is that not one of them carried out the intelligence breach acting as a recruited agent on behalf of a foreign power. They are thus not ‘spies’ in the traditional sense of the word. Instead, they were intelligence professionals who betrayed their oath to protect classified information by acting on their political or ideological beliefs. The concept of an insider leaker, however, has been dehistoricized. As early as 1963 former Director of Central Intelligence Allen Dulles coined the term ‘contrived leak’, which he identified as an appeal to public opinion via the unauthorized disclosure of classified information to the press (Dulles 2006).

Abusing their secure facilities and computer access, these leakers bested intelligence insider threat precautions – most with Cold War antecedents – and provided classified information to non-state actors such as WikiLeaks, thus providing advantage, beyond a single intelligence service, to every nation state, terrorist group, and criminal enterprise. Even if their claims about acting with noble intent are sincere, the net effect of these breaches is akin to a spy on the inside of any intelligence agency, collecting secrets in the course of their duties for onward transmission to unauthorized recipients.¹ As Dulles explained the year President John F. Kennedy was assassinated, providing secrets for publication has the same net effect as ‘betraying it to the Soviets just as clearly as if he secretly handed it to them’ (Dulles 2006). Such is the ever-present dilemma of balancing secrecy and transparency. Snowden and Manning, simultaneously the most lionized and demonized of the cyber spies, have triggered heated public debate between civil libertarians and intelligence practitioners (Albrecht 2015; Gros 2017; Van Cleave 2015), but thus far there has been more heat than light, particularly concerning estimates of damage caused by their breaches.

This article makes an original methodological contribution to the study of intelligence in international relations by offering a damage assessment framework that allows scholars and practitioners to assess the comparative significance of insider threat breaches involving national security information. While heightened political passions often attend claims of treason and betrayal, we offer a formal evaluative framework to assess damage and better understand what kind of risks insider threats pose for national security organizations. Such assessments may enable intelligence agencies to better allocate resources

¹ Noble intent by itself would not exonerate such leaks according to scholars of the ethics of treason; for example, see Hatfield 2017.

to countering different types of risk and also to avoid a perennial issue following a security breach—namely, counterproductive paranoia.

The framework identifies seven key properties of such breaches and uses a non-deterministic model that employs phronetic measurement using Likert scales and weighted proportions to structure comparative judgments about relative damage between different cases of national security information breaches. Phronetic social science places a premium on qualitatively rich judgment-based measurements rather than deterministic approaches modeled after the hard sciences (Flyvbjerg 2001; Flyvbjerg et al 2012). The comparative case-study method is employed to instantiate the framework, using the Snowden leaks and the infamous ‘Cambridge Five’ spy ring as paradigm-cases of the two major types of insider threats. The comparative case study method selects ideal-type cases as representative of a broader class for careful textured analysis (King et al 1994). Inferences are drawn from the purest cases so that a framework is established from which inferences about less pure cases can be made.

What are the case categories examined here? Insider threat actors are either *self*-tasked or receive their tasking from an *external* agency of some kind. Self-tasked insider threats are typically internally motivated and conduct their own planning and direction, while the actions of externally controlled insider threats are controlled by individuals operating externally to the institution whose information is breached. Snowden’s case is paradigmatic for the class of self-tasked cases because unlike, for example, Manning, whose cultivation by the founder of WikiLeaks, Julian Assange, might be described as having placed Manning in a semi-controlled relationship, Snowden’s activities were completely self-directed. Although separated by over half a century, the Cambridge Five spy ring is paradigmatic of externally controlled insider threat cases because their activities were carefully orchestrated by Moscow, as will be detailed below, although it would be correct to note that the ideological nature of the recruitment of the Cambridge Five since Moscow’s case officers harvested agents from already fertile soil.

It is largely due to this centralized external planning that one must consider the five together as one cooperative case; they formed a network and cannot be separated. The five did not just share the same Alma Mater, but the five knew each other; were recruited by the same KGB handler; their activities were coordinated in such a manner that their distinctive activities formed part of a larger strategy specific to that group; each were tasked in accordance with a division of labor relative to the others and they acted as each other’s warning bell when counterintelligence efforts closed in. These facts effectively merge the five into one combined case—an emblematic case of externally controlled insider threats. Considering the archetypal cases of these two type-classes helps demonstrate the categorical universality of the model—its ability to handle the entire range of cases in each sub-category.² The paradigmatic nature of both Snowden and the Cambridge Five also derives from the fact that these are, as will be argued below, egregious cases of their respective kinds and are therefore relatively less tainted by exogenous influences.

The damage assessment framework for insider threats established by this article offers scholars and others a tool to compare breach instances over time, evaluate claims about relative damage, and structure historical judgments

² For a fairly comprehensive list of insider threat cases within the US context, see Herbig 2017.

about the extent of damage inflicted by insider threat actors to national security information. The framework also empowers intelligence agencies seeking to prevent, recover from, or initiate (against its competitor), a breach in four fundamental ways. First, an objective measurement of damage gives intelligence agencies a fact-based tool that would aid it in the allocation of resources to counter the various threats against its information, sources, and methods. Alarmist declarations following an insider threat breach may initiate the misallocation of scarce resources away from areas misunderstood to be less damaging to areas actually so. Second, the framework can be used offensively to evaluate the relative value of different courses of action targeting an enemy's national security information. For example, if limited resources forced a human intelligence (HUMINT) agency into a choice between targeting two individuals with comparatively different access. This evaluation would be of a counterfactual nature, but one constrained by data rather than one's subjective bias, which potentially might lead one astray. Third, within the framework presented, some features of damage that are often overlooked receive their proper weighting, which in turn might help an organization avoid past mistakes. For example, one can see—in what follows below—the proportion of the total damage of the Cambridge Five attributable to self-defeating paranoia that took root following the discovery of the breach by CIA counterintelligence chief James Angleton. With that proportion made explicit, because of the framework offered here, the CIA might see this paranoia as something as much to be avoided as the initial breach. Finally, the framework might aid organizations by identifying and prioritizing areas of action to take immediately following a breach. That is, by assigning numerical comparisons, the framework gives organizational leaders a prioritized list from which damage mitigation efforts might be affected.

The need for a framework

Between 2011 and 2013, computer-savvy Snowden employed technical and social-engineering techniques that enabled him to exfiltrate, in the estimation of the NSA, 1.5 million highly classified British and American intelligence documents, representing sensitive transatlantic Signals Intelligence (SIGINT) and Communications Intelligence (COMINT) capabilities, methods, and partnerships (Sanger 2014; Hatfield 2018). That tens of thousands of Snowden's leaked records were of British origin speaks volumes about the intimacy of the 'Special' Anglo-American intelligence relationship and his behavior has concomitantly ruffled governmental feathers on both sides of the Atlantic (*Financial Times* 2013). The scope of Snowden's long-term damage to Anglo-American interests is far from certain, but the scale is enormous – often characterized in superlative and categorical terms, as will be explored.

Yet, it is not possible to understand the likes of Snowden in purely counterintelligence or information security terms, although surely there were internal NSA failures in these areas. The powerful concoction mixing contemporary self-identified privacy crusaders like Snowden, who claim to act on patriotic grounds, with the technical ability for one person to expose so many state secrets is a terrifying combination for intelligence and security agencies in the cyber age. The revelations from Snowden, referred to by some as a 'whistleblower,' continue to provide ample fuel for both vituperative political discourse as well as scholarly debate (Delmas 2015; Alford 2002).

In particular, the question of the scope and scale of Snowden's damage to Anglo-American national security is hotly contested. Sir John Sawers, then Chief of the British Secret Intelligence Service (also known as MI6) testified publicly before the British parliamentary Intelligence and Security Committee in November 2013, 'The leaks from Snowden have been very damaging. They have put our operations at risk. It is clear our adversaries are rubbing their hands with glee. Al-Qaida is lapping it up' (Wintour 2013). Testifying beside Sawers, Sir Iain Lobban, then-Director General of Britain's signals intelligence establishment, the Government Communications Headquarters (GCHQ), observed,

There is a complex and fragile mosaic of strategic capability which allows us to discover, to process, to investigate and then to take action. That includes terrorist cells, it reveals people shipping secrets or expertise or materials to do with chemical, biological, nuclear around the world. It allows us to reveal the identities of those involved in online sexual exploitation of children. Those people are very active users of encryption and of anonymisation tools. That mosaic is in a far, far weaker place than it was five months ago. (Wintour 2013)

Attempting to frame Snowden's actions in comparative terms, Sir David Omand, another former Director General of GCHQ and British Intelligence and Security Coordinator, averred that Edward Snowden's mass intelligence disclosures are 'the most catastrophic loss to British intelligence ever, much worse than [Guy] Burgess and [Donald] Maclean' (Whitehead et al 2013), thus providing the initial motivation for the current comparative case selection in this article.

The American versions of these arguments are likewise dire, and, like Omand's assessment, imply historical comparisons to an earlier time. General Keith Alexander, formerly Iain Lobban's direct American counterpart at NSA (and also then Commander of US Cyber Command), assessed that Snowden's treachery was 'the greatest damage to our combined nations' intelligence systems that we have ever suffered' (Sanger 2014). Michael Morell, a former Deputy Director and twice Acting Director of CIA, opined, 'I think this is the most serious leak – the most serious compromise of classified information in the history of the U.S. intelligence community' (Morrell 2013). Such a categorical pronouncement by a career intelligence professional whose stock in trade is careful analytical judgment invites academic scrutiny. Even a cursory review of the greatest traitors in the history of US intelligence would reveal that placing Snowden at the summit is a bold claim indeed. The names of Aldrich Ames, Robert Hanssen, Ronald Pelton, Edward Lee Howard, Jonathan Pollard, and Ana Montes, just to name a few, live in infamy in the corridors of the American and British intelligence establishments. If Snowden's actions, according to Omand, represent a more 'catastrophic loss' than that inflicted by the worst British spies, his actions were also atop the American heap, according to Morell and Alexander.³

³ It is notable that the overwhelming number of comparisons used thus far to understand and contextualize Snowden's impact have been to either the Cambridge Five in the UK or other notorious FBI and CIA spies in the US. Almost no observers have made mention of Snowden in comparison to the atom spies of World War II who delivered Josef Stalin the bomb. That would also be a useful comparison to test the proposed damage framework, but the current comparison is tested first because the popular narrative has shaped the comparison thusly.

Beyond the disapproving view of former senior intelligence practitioners, the United States House of Representatives House Permanent Select Committee on Intelligence (HPSCI) had similarly scathing language for Snowden and his theft of government national security information in a report which was publicly released in September 2016, as the magnitude of the breach was investigated and more clearly understood by policymakers outside of the Executive branch. Still, the categorical characterizations of Snowden's disclosures did not dissipate over time or the course of the investigation. Perhaps unsurprisingly, the HPSCI report echoed the practitioner view, again invoking historical comparison, claiming, 'Snowden perpetrated the largest and most damaging public release of classified information in U.S. intelligence history' (U.S. House of Representatives 2016). Indeed, both the Anglo-American intelligence and security establishment and their political overseers care little for Snowden's high-minded disclosures, and fear much about their negative impact. The common refrain from Washington's Executive and Legislative branches and Whitehall is that such mass disclosures are not only catastrophic in contemporary terms, they are also catastrophic in historical comparison. The consensus view of the transatlantic security establishment may be correct, but no historical parallels or comparisons have been offered as evidence for these assertions. Therefore, we seek to contribute a structured first step that, by testing the current cases, may be a tool to test other similar cases in the future.

Sir David Omand's reference to Burgess and Maclean, two of the infamous Cambridge Five was intended to cover the entire group of onetime Cambridge students who went on to serve as Moscow's eyes and ears in the heart of the British and (via liaison) American governments.⁴ This spy ring penetrated the highest echelons of the British intelligence community for nearly two decades in the mid-twentieth century. This ring, mostly stemming from Trinity College, Cambridge, were responsible for hundreds of deaths, years of wasted money and efforts, a near paralysis of Anglo-American intelligence in the early Cold War, and perhaps even seismic shifts in the East-West balance of power at the dawn of the nuclear age.⁵ They betrayed Britain's most sensitive wartime secrets, ensured that Soviet leader Josef Stalin was as well informed as wartime Prime Minister Winston Churchill on a number of crucial occasions, and nearly fractured the Anglo-American intelligence relationship, a cornerstone of the postwar security structure.

Given the competition from the Cambridge Five as the 'worst ever,' placing Snowden as first among traitors is a bold, categorical claim, and should be evaluated with the benefit of historical context as well as a nuanced framework for damage assessment. As Snowden suggested, 'We should be suspicious about the sort of overblown claims by officials about national security' (Snowden 2014).

⁴ In an email to one of the authors, dated 9 November 2014, Sir David explained that he intended his mention of Burgess and Maclean to stand for the entire group in the public discourse as much as they were the best known, and he clarified that his view that Snowden is not only worse than the Cambridge Five, but also more serious than KGB spy and former SIS officer George Blake (about whom there is regrettably not enough space to include in this historical comparison).

⁵ The atom spies that delivered Stalin the bomb would also be an apposite comparison for future inquiry and to test proposed damage assessment frameworks in historical perspective.

Surely any bold claim deserves to be carefully examined, including Snowden's own. Still, could the revelations of the former CIA staff officer turned NSA contractor actually surpass the damage done to Anglo-American intelligence by the Cambridge Five? The comparison of Snowden's and Moscow's multi-pronged penetration of American and British intelligence invites further consideration.

Elements of a damage assessment framework

A half-century on, the damage done by the Cambridge spy ring is now clear, and their motivations have also been extensively explored. Although Snowden's motivations seem evident, there remain questions about them, and the real impact of his actions is still emerging. In the rhetoric about the scope and scale of Snowden's actions, one area that requires further definition is the concept of damage itself. It is often unclear precisely what sort of damage is being alleged, especially when it is used as a term relative to other leakers or traitors, but without the benefit of historical analysis.

Damage can take many forms and the term cries out for greater descriptive specificity. Proposed new damage subcategories, or factors, for this framework are lives lost, human sources (HUMINT) and SIGINT collection methods compromised, hefty governmental financial undertaking to replace lost collection capabilities, economic or reputational damage to relevant institutions or corporations across the entire economy, stunted employee morale, redirected personnel resources 'off task' for damage assessments, geostrategic disadvantage such as shifts in balance of power, loss of national narrative in foreign policy initiatives, impaired intelligence and security liaison partnerships, and loss of future intelligence reporting streams (both human and technical). Precision and priorities represent significant challenges in measuring and ordering these considerations. For instance, lost corporate financial earnings may be relatively straightforward to categorize in terms of contracts cancelled whereas apprehending the impact of lost future intelligence collection is more challenging (Gioe 2014).

Likewise, replacing a particular intelligence collection system or platform may be expensive, but with roughly measurable direct costs to the US and UK governments. The hidden costs of fractured intelligence alliances and liaison partnerships may be unknowable, and a judgment made today may differ from that made decades later, when a full accounting of the facts and their repercussions has been made. Still, it is possible to roughly rank the various aspects of damage by their impact on the affected political community's ability to foster the conditions required for the flourishing of its citizens.⁶ To illustrate, lives lost and shifts in the geostrategic balance of power seem, through this lens, to be the most severe form of damage because the dead cannot flourish (acute failure) while the latter undermines the entire political community (systemic failure). This is followed by impaired partnerships and alliances, which are less systemic, and lost or compromised intelligence sources or methods, with national and corporate financial considerations, loss of diplomatic and national narratives, and intelligence community morale at the lowest tier.

⁶ It is beyond the scope of this paper to offer a justification for this broadly Aristotelian view of the purpose of the state. But for an explanation of this view as it relates to insider threats, see (Hatfield 2017).

Base case (a): Cambridge Five Comparison case (b): Snowden		Qualitative-Comparative Damage Framework				<u>Factors</u> 1. Lives lost (often a function of the timeliness of intelligence) 2. Sources & methods compromised (a function of the placement & access a leaker has) 3. Cost of replacing lost collection capabilities 4. Economic or reputational damage done to relevant institutions or corporations 5. Stunted employee morale 6. Redirected personnel resources for damage assessments 7. Geostategic disadvantage a. Shifts in balance of power b. Loss of national narrative in foreign policy initiatives c. Impaired intel liaison d. loss of future intelligence reporting streams
Factor measurement / magnitude (x)		Comparison to Base		Weighted Comparison		
(x)	(y)	(b)	(a)			
Extremely costly in comparison - 5		0	25			
Very costly in comparison - 4		0	25			
Moderately costly in comparison - 3		0	25			
Slightly costly in comparison - 2		0	25			
Not costly in comparison - 1		0	25			
		0	25			
Factor Significance (y)		N/A	N/A	N/A	N/A	
Extremely significant in comparison - 5		0	25			
Very significant in comparison - 4		0	25			
Moderately significant in comparison - 3		0	25			
Slightly significant in comparison - 2		0	25			
Not significant in comparison - 1		0	25			
		Result =		0	250	

Figure 1. Qualitative-comparative damage framework.

Albeit an imprecise guide to understanding the various types and severity of damage, by applying this conceptual framework across a comparative historical tableau, more accurate insights may emerge and more useful historical comparisons may be offered. In this way, categorical claims may be validated, or alternatively, may be tempered. At the very least, the questions should be sharpened and the debate both elevated and historically informed.

Damage assessments can be considered either absolute or comparative, depending upon whether they claim to provide an objectively static measurement or simply the extent of damage relative to a base case. The framework offered here is of the latter variety. That is, it is not meant to establish an absolute scale against which past and future insider threat breaches can be fixed. Such a scale would have to abstract away from the historical specificities surrounding any particular breach even though it is only within its context, which cannot be replicated, that its significance to national security can be reliably judged. By contrast, the framework put forward here seeks to retain contextual nuance and does so partly by limiting its ambitions to that of providing a mechanism by means of which insider threat breaches can be compared.

Figure 1 illustrates the damage assessment framework offered in this paper. It first lists the two cases being compared: the Cambridge Five (a) and the Snowden leaks (b). It further specifies two factors that will be used to make comparative judgments of the Snowden leaks (b) when compared to the base case (a). These two factors are magnitude of cost (x) and significance (y), which are both measured by means of Likert-scales using Extremely (5), Very (4), Moderately (3), Slightly (2), and None (1), as their respective Likert terms (Myers et al 2013). On the right-hand side of the framework the aforementioned factors are listed (1-7). The seventh factor has been subdivided into four sub-factors which are to be examined individually. The factor numbers act as a traditional y-axis, with (x), (y), (a), and (b) acting as a traditional x-axis. As such, the nomenclature x1 corresponds to the cell in the x-column that aligns with factor 1 (lives lost), and so on for the remaining cells in the (x) and (y) columns. Therefore, using the model consists of filling in two columns (x) and (y) in the following manner. For (x1) one asks: ‘How costly, in terms of magnitude, were the lives lost as a result of Snowden’s leaks when compared to those of the Cambridge Five?’ Using the Likert scale on the left (x), one selects a category and records its corresponding number (1-5) in (x1). In each of these (x) judgments one must consider the measured cost but not as an absolute

value but rather in its relation to the base case. So, in the case of Snowden, since no lives have been lost due to his revelations and hundreds of lives were lost from one of the Cambridge Five's treachery alone, that of H.A.R. 'Kim' Philby, more about this below, this cell would almost certainly receive the lowest Likert category 'Not costly in comparison – 1'. For the (y) column one asks a different question pertaining to the significance of the very factor being judged (in the above case, again, this is lives lost) relative to its significance in the base case. Thus for (y1) one asks: 'How significant are 'lives lost' in Snowden's case compared to that category in the case of the Cambridge Five?' This question is crucial for measuring the circumstantial context that surrounds each case, specifically when historically divergent cases are compared. Using the Likert scale on the left (y) one selects a category and records its corresponding number (1-5) in (y1). If one considers the significance of 'lives lost' as a category of damage to be equal in both cases one would input a '1' in (y1) since this would entail that this category carries no more (or less) weight in the Snowden case as that of the Cambridge Five.

Columns (x) and (y) must be considered separately to allow for historical comparisons wherein factors are weighted differently for contextual reasons. For example, during war, a breach which costs five lives may barely register as significant given the tremendous human-costs associated with war in general. But during peacetime this cost may be deemed far more costly. This is captured in the framework by separating the magnitude from the weighted importance or significance. In this case, a case comparing a peacetime scenario against a wartime base, (y1) might receive a higher Likert scale evaluation. Similarly, with respect to (x). Consider the case where the five individuals killed are extremely important people in the comparison case (b) but ordinary people in the base case (a). In that case, (x1) might receive a higher Likert scale evaluation. Thus, separating the relative (x) and (y) measurements allow for historical context and depth to be captured by the framework.

Once columns (x) and (y) are populated, columns (a) and (b) can be automatically derived. Within this framework, column (b) equals the product of (x) and (y) for that respective factor, while column (a) equals the difference between (b) and the maximum possible Likert-product (25). For example, using the judgments for (x1) and (y1) above for the factor 'lives lost,' if (x1) evaluates to '1' and (y1) evaluates to '5' then (b) evaluates to '5' ($1 * 5$) and (a) evaluates to '20' ($25 - (b)$). Since (a) and (b) correspond to the base case (e.g. Cambridge Five) and the test case (e.g. Snowden) respectively, the results for that factor can be read as saying that at least in terms of lives lost (a1) and (b1) the assessed damage that resulted from Snowden's leaks are dwarfed by that which resulted from the activities of the Cambridge Five.

A phronetic social science approach governs several aspects of the use of this model. Phronetic social science, as described by Oxford's Bent Flyvbjerg, is judgment-driven and qualitative in nature (Flyvbjerg 2001; Flyvbjerg et al. 2012). Thus, the Likert scale judgments are designed to allow users to draw from the contextual depth of historical knowledge available to them when determining which category applies to each respective comparative

judgment. Following King, Keohane, and Verba (1994, 77-79), we define causality within this framework as the difference between a resultant factor-coefficient or measurement when an historical case y_I^h (where h denotes the historical case and I denotes the presence of insider threat activity) and a counterfactual case y_N^c (where c denotes its counterfactual nature and N denotes that no insider threat activity exists) are compared *mutatus mutandis*.⁷ If, for example, the use of the framework finds that when compared to a counterfactual historical case where no insider threat activity is present there is an increase in the evaluated level of damage (e.g. lives lost) when insider threat activity is present, then that activity is understood to have been causally efficacious for that factor.

In keeping with the phronetic social science approach that underlies this framework, the result-statistics, calculated as a sum of columns (a) and (b) respectively, once all the Likert judgements are made, are not meant to be used in an algorithmic or deterministic manner. Rather, they make explicit what is often implicit in comparative judgements, allowing for researchers to identify why, and on what variable(s), they disagree. The ultimate aim of the framework is to avoid rash judgments which are often made by people (e.g. intelligence agency directors) whose lives have been altered by the very breaches they are asked to dispassionately evaluate. Due to their standing within the profession, distorted or impassioned claims on the part of such individuals carry more weight than they otherwise should. Using the framework offered above helps avoid this pitfall.

It is important to highlight the innovative nature of our methodological contribution, especially within the context of Intelligence Studies. We offer a formal methodological approach to the assessment of relative damage in an area of academia that has been criticized as being, in the words of Christopher Andrew, 'under-theorized' (Andrew 2004). While it is common within Intelligence Studies to employ historical, comparative, and even philosophical methods (Gaspard 2017), structured analytical techniques have mostly been confined to discussions of analytical bias within the context of intelligence analysis (Pherson and Heuer 2021) and counterintelligence (Heuer 2009), while statistical modeling of various kinds has largely been met with skepticism, even in areas most amenable to numerical treatments, such as military intelligence (Bang 2016). Indeed, rather than being merely absent, formal analytical models are sometimes positively discouraged (Smith 2017). By contrast, the framework offered here demonstrates the power that structured methods can bring, when appropriately applied to questions of importance within Intelligence Studies. It does so without committing to reductionist epistemological impulses rightly feared by scholars within the field.

⁷ *Mutatus mutandis* because every historical case contains unexplainable endogenous variation which needs to be eliminated from the overall comparison (for both terms y_I^h and y_N^c) lest it potentially overwhelm the measured accuracy of the comparison. King, Keohane, and Verba (1994, 80-81) describe this elimination procedure within the context of the definition of causality as one of measuring and accounting for 'random causal effect.' See King, Gary, Robert O. Keohane, and Sidney Verba (1994) *Designing Social Inquiry: Scientific Inference in Qualitative Research*, Princeton: Princeton University Press.

Self-tasked insider threats: the case of snowden

A common starting point is difficult to find in the Snowden affair. Snowden and his supporters have stoutly maintained that the question of damage is a canard because none has been proven to their satisfaction. For instance, Glenn Greenwald holds that none of the Snowden revelations ‘even remotely jeopardize’ US national security, although he does not express the criteria on which he bases this assertion (Maass 2013). Echoing his journalist-publicist’s line, Snowden asserted, ‘The risks that have been threatened, the risks that have been played up by the government have never materialized. We’ve never seen any evidence of even a single instance of specific harm’ (Snowden 2014). Even if true, of course, this raises the question of future or potential harm and Snowden’s responsibility in it.

On the other hand, the NSA has countered that America and its allies are more vulnerable because terrorists are changing their communications methods in response to his disclosures (Ledgett 2014).⁸ Former NSA Director Admiral Michael Rogers has not shied away from addressing the question of damage from his optic: ‘For those who would argue that the media leaks have had no impact, I would argue you don’t know what you’re talking about. I’m watching groups change their behavior. I’m watching groups talk about the disclosures and say, ‘Look, we can’t use this because the Americans are onto it’’ (Romano 2014). This is illustrative of the fear on the part of Anglo-American intelligence agencies in that previously successful methods of tracking terrorists and other security threats have been compromised, making keeping tabs on the malign actors that much harder – if possible at all – potentially only realizing plots after they have come to fruition.⁹

This change in the method of terrorist and criminal communications is part of a larger movement toward boutique but booming Internet and digital security commercial offerings. For example, the communications security company Silent Circle offers an encryption application, which provides enhanced data security. As one researcher noted, ‘Although Silent Circle doesn’t provide specific numbers, it saw a ‘huge increase’ in subscriptions to its private phone and text service after Snowden’s disclosures.’ Silent Circle co-founder Jon Callas disclosed, ‘Snowden’s leaks were a real boon for us’ (Aid 2014). Surely this is not to say that most, or any, clients of Silent Circle or any other encryption provider are terrorists or criminals. Still, the diffusion of sophisticated encryption technology is increasingly available to increasingly aware users wishing to defeat communications intelligence (COMINT) collection and the ongoing battle between Silicon Valley and law enforcement is indicative of this trend.

Further, the awareness of the apparent necessity of such services is deeply troubling to Anglo-American intelligence professionals. Terrorist elements, such as al-Qaeda, have offered their own data encryption protocols long before Snowden joined NSA. One Internet security protocol, Mujahedeen Secrets, was

⁸ According to NSA Deputy Director Rick Ledgett, there were 54 instances in which NSA programs in question helped foil terrorist attacks (12 US-focused, 41 focused at allies). See his response to Snowden’s TED Talk in Ledgett 2014.

⁹ This will, inevitably, result in cries of intelligence failure and calls for further organizational reforms like the creation of a Director of National Intelligence.

publicly deployed by al-Qaeda for any sympathizer or associate to use within Microsoft Windows in 2007, and revised in 2008 (Schmitt 2013). In the wake of the Snowden disclosures, however, the Internet technology firm Recorded Future revealed that the Snowden leaks directly caused al-Qaeda's crypto product innovation. Indeed, al-Qaeda specifically cited Snowden's leaks in a directive to take such cryptographic precautions especially regarding smart-phone use (Ahlberg 2014).

Although missing small warnings may result in tactical – if not strategic – surprise (as in the case of the Japanese attack on Pearl Harbor in 1941), most allegations of damage appear most closely linked to the idea of public danger, specifically, a weakening of Anglo-American security posture with particular regard to counter terrorism capabilities. If most terror attacks result in the loss of innocent life, this must rank at the top of the damage framework. The crux of the argument put forth by the various heads of the Anglo-American security and intelligence establishment is that American or British intelligence or security services may miss a potentially vital clue that may impair official efforts to disrupt or prevent a catastrophic terrorist attack. As the 9/11 Commission famously observed, connecting the dots is an important part of intelligence analysis. It follows that reducing the amount and quality of data that counterterrorism analysts have to work with will impede their efforts to prevent terrorism. Testifying before the Senate, then-Director of National Intelligence James Clapper asserted, 'People's lives are at risk here because of data that Mr. Snowden purloined' (Cole 2014).

To synthesize the arguments of Lobban, Rogers, and Clapper, Snowden's revelations have put lives at risk by enabling malign actors to avoid detection by US (and British) intelligence agencies. Michael Morell put it this way: 'What Edward Snowden did has put Americans at greater risk because terrorists learn from leaks and they will be more careful, and we will not get the intelligence we would have gotten otherwise' (Morrell 2013). This argument is what links the damage of missed or lost intelligence to a higher level of damage: lives lost. Of course, this is not simply a binary proposition; timeliness is a key factor in the usability of intelligence. Insights delivered too late might as well not have been provided at all. The issue of timeliness (and thereby relevance) was addressed by GCHQ via Britain's *Telegraph* newspaper:

Britain's spies now take three times as long to crack terrorist communications thanks to the Edward Snowden leaks of GCHQ techniques. Experts at the intelligence agency need up to six weeks to 'deliver the magic' when tasked with tracking and monitoring targets... The expert, known only as Simon, said before Snowden it took him a fortnight to 'deliver the magic'. Now it takes six weeks. Another said it had 'made my job 1000 times more difficult'. (Moore et al 2014)

In broader terms, as Iain Lobban observed, counterterrorism is not the only thrust of intelligence services. Counter-proliferation, counter-narcotics, and counter-intelligence are also within the remit of intelligence and security services. Snowden's leaks have revealed the targets of Anglo-American intelligence collection as well as the methods by which they are collected against.

Assuming that the US Congress wished to attempt to replace the technical capabilities that Snowden compromised, then-Chairman of the Joint Chiefs of

Staff, General Martin Dempsey, offered, 'The mitigation task force will need to function for about two years, that's the magnitude of this challenge, and I suspect it could cost billions of dollars to overcome the loss of security that has been imposed on us' (Capra 2014). The private sector outlook is also bleak, but it is disputed as to who is to blame. A policy paper by the New America Foundation Open Technology Institute found that the US technology sector suffered substantial lost revenues. These lost profits stemmed from the erosion of international trust in the security of their products due to the relationships, disclosed by Snowden, between American technology companies and the US intelligence community. This paper calculates losses for the US cloud computing businesses ranging from the tens to hundreds of billions of dollars (Kehl 2014).

It remains, however, hotly contested whether Snowden ought to be blamed for disclosing the nature of these relationships, or whether the NSA is to blame for having them in the first place, as the Open Technology Institute does. Other officials have privately muttered that European boycotts of American technology companies on the basis of their cooperation with lawful intercept operations and the Patriot Act ring hollow and are actually thinly veiled protectionism. Further, most other industrialized countries, initially in a rush to express outrage over the Snowden revelations, have similar arrangements with their own domestic telecommunications firms (Amble 2013). How one might calculate and quantify where the damage in this case lies, and where the blame falls, depends on the view one holds of industry's patriotic responsibilities (and compliance with US law) on one hand, or a more global perspective with data security and privacy for all on the other hand.

Placement and access are two primary considerations when assessing the value of an insider threat as well as understanding how much damage he can cause if he were to abuse the trust required by his employment. Notably, it is not asserted here that Snowden was a witting agent of a foreign power at the time of his disclosures. But the information he stole did reach (and would be useful to) adversary countries. Thus, a systematic comparison of placement and access is essential in applying a comparative damage framework for Snowden and the Cambridge Five. Snowden worked at both CIA and NSA, and thus had first-hand access to the two key players in American foreign intelligence collection. Moreover, through the NSA's close relationship with GCHQ, Snowden was also able to pilfer tens of thousands of GCHQ documents. This may indeed seem an impressive scope. However, it is not nearly as wide-ranging as the breadth of coverage provided to the KGB by the Cambridge Five – Five individuals, but a single network (Boyle 1979).

When taken in total, the Five personally worked for the British Secret Intelligence Service (MI6), the British Security Service (MI5), GCHQ, the Government Code and Cypher School (the wartime predecessor of GCHQ at Bletchley Park), the Special Operations Executive (SOE), the British Army Intelligence Corps, the Foreign Office, the Treasury, Parliament, the Cabinet, and the Crown itself. Further, through various special liaison relationships, the Five were also able to collect information from the CIA and its wartime predecessor, the Office of Strategic Services (OSS), the NSA and its predecessor, the Armed Forces Security Agency (AFSA), the wartime Supreme Headquarters Allied Expeditionary Forces (SHAEP), and the FBI. In short, if a US or British

intelligence, security, diplomatic, or political body were not penetrated to some degree by at least one member of the Cambridge Five, it was the exception that proved the rule.

If a particularly sensitive level of accesses is good, being able to move along to even greater access is better. One of the most striking commonalities between Snowden and the Cambridge Five is how each maneuvered to increase their access to ever more sensitive classified material. In 2010 Snowden left CIA and was hired by Dell to work as an NSA contractor in Japan. By 2012 Snowden was still with Dell but took a job transfer to Hawaii. Once he was fully committed to his chosen path, Snowden attempted to join the NSA's elite hacking organization, Tailored Access Operations (TAO) (Peterson 2013). Although ultimately unsuccessful joining TAO, Snowden subsequently took a position with defense contractor Booz Allen Hamilton in order to increase and diversify his access. As recounted by James Bamford: 'There was one key area that remained out of his reach: the NSA's aggressive cyber warfare activity around the world. To get access to that last cache of secrets, Snowden landed a job as an infrastructure analyst with another giant NSA contractor, Booz Allen. The role gave him rare dual-hat authority covering both domestic and foreign intercept capabilities (Bamford 2014).' For one with Snowden's purpose, this was a prize perch. However, as an individual, Snowden could not corroborate the reporting of other agents in a network, nor could provide insight into the perspective of other agencies looking at a common problem from another angle.¹⁰ In contrast, KGB conducted the Cambridge Five orchestra to harmonize with each other, some providing the deep bass notes, others descants of winds, and all contributing to a common score. The ability to validate both the source and his information in this way is a rare intelligence feat.

Access and placement are, of course, not ends unto themselves. They are means by which an agent (or insider) may purloin as much classified or sensitive information as may be helpful to his cause, or that he may receive tasking to procure. In the case of sheer volume of material, Snowden's betrayal single-handedly exceeded the remarkable volume of intelligence procured by the Cambridge Five and it is worth taking stock of the quantity. Snowden made off with circa 1.5 million NSA documents, according to the HPSCI investigative report (U.S. House of Representatives 2016). Intelligence historian Christopher Andrew and his KGB defector co-author Vasili Mitrokhin offer the most authoritative estimates of the volume of material stolen by the Cambridge Five on behalf of the London office of the KGB's wartime predecessor, the NKVD¹¹:

During 1941 London was easily the NKVD's most productive legal residency. According to the Center's secret statistics, the residency forwarded to Moscow 7,867 classified

¹⁰ Despite Snowden's coup by landing at NSA's outpost in Hawaii, his remained a singular effort.

¹¹ The KGB, the Committee for State Security, was called various things at various times, including NKVD from the mid-1930s through the end of the Second World War, the balance of this article will simplify this nomenclature by referring the Soviet intelligence and security apparatus as the KGB, although this name change did not occur until 1954 and was officially dissolved in 1991.

political and diplomatic documents, 715 on military matters, 127 on economic affairs and 51 on British intelligence. In addition it provided many other reports based on verbal information from the Five and other agents. (Andrew 1999)

Andrew further notes: 'For 1942 alone Maclean's documents filled more than forty-five volumes in the Center archives' (Andrew 1999). For totals that include the postwar period as well, Andrew, as official historian of the Security Service, records in the authorized history of MI5: 'The Center calculated that, since their recruitment in 1934-5, Philby, Burgess, and Maclean had supplied more than 20,000 pages of 'valuable' classified documents and agent reports' (Andrew 2009). In the pre-digital age, such a volume of intelligence production is staggering.

Numbers do not tell the whole story and, in isolation, are a poor predictor or measure of damage, notwithstanding Stalin's reputed observation that quantity has a quality all its own. Further, it is difficult to compare the total pilfered products in terms of numbers of pages, volumes, documents, digital records, and network diagrams on PowerPoint slides.¹² In terms of qualitative analysis, it is also useful, but difficult, to determine how valuable Snowden's documents are to those who would like to know that information. All of Snowden's documents are likely not of interest to terrorists, criminals, and geopolitical rivals in equal measure. If the 1.5 million figure is the correct one, there is no possible way Snowden could have actually reviewed more than a small sample of them, nor are the majority available (as yet) for public review. This is more reminiscent of Chelsea Manning's indiscriminate hoover method than a careful spy considering what might please his handlers in response to their tasking.

Conversely, the Cambridge Five knew precisely what their handlers required and sought those specific documents or memos related to a particular issue at hand. Additionally, as their case officer Yuri Modin pointed out, not all material of interest is in documentary form; some material is passed verbally: 'When people say that the only agents of any value are those that can lay their hands on crucial documents, they are wrong' (Modin 1995). A savvy practitioner of the art of intelligence, Modin is correct. Considering the case of Snowden – beyond counting documents – it is unknown what he told his interlocutors in Hong Kong or Russia which relates to the capabilities or targets of Anglo-American intelligence.

If one can posit that damage and value have a corollary relationship, it follows that intelligence value to one side is the photonegative of damage to the other side. Thus, having reviewed aspects of Snowden's damage, it is useful to review exactly what was provided to the KGB by the Cambridge Five; and, to attempt to determine its utility to its recipients in comparison to Snowden.

Externally controlled insider threats: the Cambridge Five

Perhaps the most infamous of the Cambridge Five, Harold Adrian Russell 'Kim' Philby likely did the most damage, out of his contemporaries, to British

¹² On the Cambridge Five side, it is unknown how many pages are in a 'document' or a 'volume'. In relation to Snowden, it is unknown how many pages are in a digital record, and, in any case, it is probably not constant.

national security. Philby's betrayals were unique amongst his compatriots in that his actions can be directly linked to loss of life in several instances (Macintyre 2015; Macintyre 2018). Philby is often placed atop the Cambridge Five because his access was transatlantic in scope and compromised CIA covert action and collection efforts, as well as those of the Armed Forces Security Agency (AFSA), the predecessor of the National Security Agency. Although Philby was the last of the Cambridge Five to secure a sensitive position within the British establishment, he ultimately surpassed his colleagues in damage, calculated in terms of lives lost, strain on the Anglo-American Special relationship – particularly the devastating paranoia his betrayal induced in CIA's chief molehunter James Angleton, and compromising joint operations which, arguably, may have led to a shift in the relative power of East and West in the early Cold War. Detailing the exploits of – and hence damage by – Kim Philby is the subject of a vast literature, but some highlights are in order to illustrate the broad sweep of Philby's impact on Anglo-American intelligence and national security.

Convinced at Cambridge that he must 'devote his life to communism', Kim Philby joined the SIS in 1941, after brief service in the British SOE with fellow Trinitarian and Soviet agent Guy Burgess. Although Philby had consequential impact during the war years, his post war exploits were his most productive. Philby was intelligent, with apparently higher levels of social and emotional intelligence than scholastic aptitude. He could persuade, cajole, and charm his way into access he should not have had, and professional positions that cracked open SIS operations against the Soviet Bloc. Using his immense charm and social connections, Philby managed to jockey his way up through the SIS bureaucracy, securing for himself, and the KGB, the position as Chief of Section IX, Soviet Affairs. In that position, Philby was tasked with penetrating the Soviet Union as well as, along with MI5, frustrating KGB and Soviet Military Intelligence (GRU) attempts to penetrate SIS operations (Macintyre 2015).

In contemporary terms, Philby had both a positive intelligence as well as a counterintelligence mandate, and he used both to maximum effect. Philby's colleague later observed: 'At one stroke he got rid of a staunch anti-communist [Felix Cowgill, Philby's erstwhile superior and presumptive designee for head of section IX] and ensured that the whole post-war effort to counter communist espionage would become known in the Kremlin. The history of espionage offers few, if any, comparable masterstrokes' (Andrew 2009). Ben Macintyre vividly illustrated: 'The fox was not merely guarding the hen house, but building it, running it, assessing its strengths and frailties, and planning its future construction' (Macintyre 2015).

The full scope of the damage afforded by Philby's 'masterstroke' is difficult to quantify but is regarded as immense by his allies and adversaries alike, as well as his biographers and intelligence historians. Philby's first opportunity to make an impact in the great game came in the person of KGB officer Konstantin Volkov, formerly of the British Desk in Moscow's KGB headquarters. Once posted to the Soviet Consulate in Istanbul, Turkey, Volkov defected to the British in August 1945. In his initial meetings with British representatives, Volkov warned of a mole in British intelligence, and two others in the Foreign Office. Upon receiving the report from Turkey, an alarmed Philby

immediately knew the unnamed mole was he, and nearly as disconcerting, the Foreign Office traitors must be fellow Cantabrigians Burgess and Maclean. Philby informed the Soviets and played for time in SIS, thus providing the KGB with time to drug and extricate their wayward officer back to Moscow, where he was executed. As Modin recalled, 'The lamb had come to the slaughter. ... Suffice it to say that he was summarily tried and shot' (Modin 1995).

The death of Volkov, while tragic in itself, had far reaching consequences for Anglo-American national security. The identity of Volkov's moles went to his grave with him. If the British had identified the moles in 1945, several of the Cambridge Five would almost certainly have been arrested at the end of the War. Instead, Philby's treacle-footed ploy ensured that he, Burgess, and Maclean could continue to undermine British intelligence and security for another six devastating years. Greater loss of life was in the offing.

The year after Volkov's execution, Enver Hoxha, the effective Albanian wartime communist guerilla leader, had seized the Albanian presidency and charted Albania's ship of state into Soviet satellite waters. Although the SOE had armed and trained Hoxha's irregulars during the recent war, these same men, only a short time later, were aiding Greece's communist partisans who were bleeding the British-backed Greek loyalist forces.¹³ Moreover, Anglo-American policy planners were disconcerted to discover that the Soviets were planning to develop a submarine base at the Karaburun Peninsula near the port of Vlorë. Soviet Naval bases in the Adriatic would challenge the allies Sea Lines of Communication in the Mediterranean. Soviet military advisors were already training Albanian security forces.

Two years later, in June 1948, Tito's Yugoslavia split off from the Soviet Bloc. This suddenly geographically isolated Hoxha from his Soviet patrons. Yugoslavia would now serve as a buffer between Albania and the rest of the Soviet Bloc and would limit Moscow's ability to interfere in Albania. Given these conditions, the Anglo-American policy officials directed their intelligence services to take action to remove Hoxha from power through a major paramilitary operation. It was hoped that Albania could be prised away from Moscow's grasp, thus robbing Stalin of a client state and, consistent with the Truman doctrine, confront communism by arming resisters.

Once the green light was given for Operation BGFIEND (known in the UK as 'Valuable') British and American intelligence officers scoured displaced persons camps in Greece, Italy and Turkey looking for Albanian anti-communists. The allies did not have to dig too deeply and were able to form a force of primarily nationalists and Royalists who were willing to stake their lives in the plan. A training base was established on Malta. CIA and SIS believed that a large-scale parachute drop of expatriate Albanian Royalists into the nationalist enclave Mati region of central Albania would ignite a popular revolt against Hoxha (Weiner 2007). Ideally, this would serve as a proof of concept for popular outbursts against other Communist satellites in the Eastern Bloc. Even

¹³ Hostilities turned from proxy war to direct confrontation when Hoxha's coastal batteries had begun firing on British Naval vessels in the Adriatic and, on 22 October 1946, two British destroyers, *Saumarez* and *Volafge*, were heavily damaged in the Corfu channel and 43 sailors were killed after striking Albanian sea mines.

limited success would divert Soviet resources to Albania that may have been bound for neighboring Greece as well as deny Albanian sanctuary to Greek communist fighters. Finally, while a successful operation to separate the geographically vulnerable Albanians from the Soviet Bloc may have had an out-sized propaganda value (and this was mentioned at the time as a desired outcome), outright failure was the immediate result (British National Archives).

Kim Philby was intimately involved with this covert action from the first. During its planning stages, British Joint Intelligence Committee (JIC) Chairman William Hayter led a delegation to Washington to secure American participation in the operation; Philby accompanied him. A few years later, once the operation was underway, Philby was then serving as chief of SIS liaison in Washington, D.C. Between 1949 and 1952, from his perch at the center of Anglo-American intelligence operations, Philby passed amphibious infiltration and parachute drop zones and corresponding dates times to his Soviet handlers, who, in turn, informed Hoxha's forces. Agents dropped into Albania, as well as those who came ashore via waterborne insertion, were almost always greeted by hostile security forces and usually lost their lives on the spot or were executed after show trials. Philby's role was key in providing 'vital information about the number of men involved, the day and the time of the landing, the weapons they were bringing and the precise program of action... The Soviets duly passed on Philby's information to Albanians who set up ambushes' (Modin 1995). Damage in terms of human cost has been estimated at 300 lives lost.

From a counterfactual perspective, it is hard to assert that Philby's treachery is the lone cause of the failure of the Albanian covert action. Contributing to its bloody result was likely the numbers of persons in the Albanian émigré community involved, numbering well into the hundreds, in addition to those who got wind of the plan through the screening and recruitment process. Thus, in addition to the unfounded assumptions about subterranean local support once underway, this operation may have also foundered on the rocks of operational insecurity regardless of what Philby passed to his Soviet handlers. Nevertheless, the Albanian agents may have at least had a fighting chance of a popular groundswell, at the most, or, in the least, perhaps the ability to quietly blend into the landscape and return home once it was clear no popular uprising was going to catch on. In direct terms, Philby's actions ensured that the Albanian agents never had a chance. In indirect terms, the failure of the Albanian operation ensured that confronting communism was going to be a harder slog than anticipated. And, at the highest level of abstraction, Anglo-American joint intelligence operations had a net record of failure at a time when it was uncertain on both sides of the Atlantic whether or not to continue the close wartime intelligence collaboration – the abysmal failure of the Albanian operation was a clear negative against Cold War joint operations.

By 1951 the British had all but abandoned the Albanian operation. Yet, that same year, the painstaking top secret VENONA operation was beginning to provide tantalizing clues as to who might be a long-serving Soviet agent within the British Foreign Office, codenamed 'Homer'. In 1943, out of a distrust of Stalin, the US Army Signal Corps – in partnership with the British and Australians – began to intercept Soviet diplomatic and military cable traffic, codenamed VENONA. Their big break came when a Soviet message was encrypted using a One Time Pad that had been used before.¹⁴ This opened the

door to exploitation of years of previously unintelligible back traffic. Joint work on the decrypts began in 1947 and, as a product of this careful detective work the transatlantic allies began to identify Soviet agents in the west as early as 1948. The scale of the collection was as far-reaching as the Soviet penetration of the US and British governments. On the American side VENONA revealed that Soviet agents had penetrated the wartime Office of Strategic Services (OSS), the Treasury and State Departments, and even the White House.

VENONA was so sensitive that it is possible that perhaps even President Truman was not briefed on it specifically. Yet, in the context of the transatlantic postwar SIGINT arrangement, (the UK-USA Agreement of 1946) the British were informed. 'Whereas wartime Ultra was primarily a British success shared with the Americans, the first major SIGINT breakthrough of the Cold War was an American success shared with the British,' noted Christopher Andrew (Andrew 2009). Specifically, the brilliant AFSA codebreaker Meredith Gardner shared his findings with the local SIS liaison officer, Kim Philby. If the VENONA program itself was promising, the counterintelligence ramifications were staggering. In addition to exposing several Soviet atom spies from the Manhattan Project, including Ted Hall, David Greenglass, and Klaus Fuchs, VENONA derailed the Cambridge Five, but not before Philby could ensure his compatriots escaped arrest. Thanks to Kim Philby's careful cultivation of Gardner, he was able to piece together that the VENONA intercepts were pointing toward Donald Maclean. Philby was thus able to tip off Maclean that the net was closing in around him. Maclean, accompanied by Guy Burgess, fled to Moscow in May 1951, casting public suspicion on Philby as the 'Third Man'. Although Philby was forced out of SIS after this affair, he was let go with a golden handshake, and the promise of occasional work.

Over a decade later, many Americans still believed that Kim Philby, a confidante of CIA counterintelligence chief Angleton, was in fact the Third Man. Only a week before Philby's defection in January 1963, MI5 Director General Roger Hollis and Sir Dick White, Chief of SIS, decided to tell the Americans that, although Philby was a traitor, he was a wartime traitor only. Their understanding of Philby's treachery spanned only 1936 to 1946, as this was the extent of Philby's confession to his friend and SIS colleague Nicholas Elliott. Not only was Elliott convinced, so too were White and Hollis. To tie up this essentially wartime loose end, Hollis wrote to FBI Director J. Edgar Hoover on 18 January 1963:

In our judgment, [Philby's] statement of the association with the [KGB] is substantially true. It accords with all the available evidence in our possession and we have no evidence pointing to a continuation of his activities on behalf of the [KGB] after 1946, save the isolated instance of Maclean. If this is so, it follows that damage to United States interests will have been confined to the period of the Second World War. (Andrew 2009)

¹⁴ One Time Pads are theoretically unbreakable because they are completely random. No pattern would be evident for a cryptanalyst to break into. As their name implies, however, they are meant for a single use only. There is temptation to reuse them when there are not enough OTPs available to keep up with message traffic demands.

The whole truth revealed only months later after Philby boarded the *Dolmatova* for Odessa, Ukraine, would be even more devastating. Indeed, Philby's defection would have prompted an even more embarrassing revision of the SIS and MI5 damage assessment of his treachery. Logically, this too would have to be shared with the Americans, adding over a decade of spying to Philby's rap sheet, and substantially downgrading American perceptions of British security continuing in the early 1960s. Indeed, lamenting the woeful extent of British intelligence background checks before access to classified information, Allen Dulles complained, 'the fact that one wears the 'old school tie' is not enough' (Dulles 1995).

In the twilight of his life, Kim Philby had a remarkable ability to blind himself to the bankruptcy of the Soviet system, writing, 'As I look over Moscow from my study window, I can see the solid foundations of the future I glimpsed at Cambridge' (Andrew and Vasili 1999). Correspondingly, Snowden appears to have the same ability for self-delusion, claiming during his brief stay in China's protectorate of Hong Kong that his hosts had 'a spirited commitment to free speech and the right of political dissent' (Borger 2013). Philby died in Moscow in 1988, having taken on a Russian wife, but not the language (Philby 1999). Deluded to the last, Philby stoutly maintained that he was an officer of the KGB; he was never more than its agent. The recipient of a lavish state funeral, Philby is the only member of the Cambridge Five to remain in Soviet soil, repudiating Britain to the last.

Art historian and Soviet agent Anthony Blunt, elder statesman of the Cambridge Five, penetrated the British Army's Intelligence Corps, the Security Service (MI5), and even the inner sanctum of the House of Windsor thanks to his post as surveyor of the Queen's pictures (Carter 2002). Although known to be a Marxist during his time at Trinity College, Blunt was nevertheless commissioned into the Army INT Corps in 1939 and served in Europe during the 'Phoney War' before joining MI5 the following year. Thanks to his post in MI5, Blunt was knowledgeable about the British codebreaking effort at Bletchley Park, and used his access there to facilitate passage of Ultra intelligence to the Soviets. Part of this was due to his recruitment of a sub-agent, Leo Long, working at Bletchley, as well as providing courier services between fellow Trinitarian John Cairncross, also a Bletchley codebreaker, and the KGB. Although the Soviets were wartime allies, the sensitivity of Ultra intelligence inveighed against sharing the source of the intelligence with Stalin because any indication that the German codes were penetrated would invite the Germans to change their encryption practices. On May 26, 1944, shortly before the allied landings in Normandy, codenamed OVERLORD, Blunt provided the KGB with the allied deception plan, codenamed FORTITUDE, including MI5's Double-Cross system – its use of double agents designed to fool the Germans about the intended timings and locations of the cross-channel invasion (Andrew 1990; Andrew 2009).

After the war, Blunt remained with MI5. He found that he had a talent for innovating surveillance techniques and proposed new and improved tradecraft doctrine for the 'watchers', MI5's surveillance teams, as well as for MI5's own agents. MI5 leadership institutionalized Blunt's contributions as standard operating procedure. He then provided his new security tradecraft textbook to the KGB. According to Modin, 'They never dreamed that a mole inside their

surveillance services had taught us every detail of their methods' (Modin 1995). In his memoir, Modin provides a remarkable account of the damage that Blunt did to the Security Service specifically, and British security generally:

Through Blunt, the Soviet Embassy in London was always informed well in advance of any actions against us contemplated by British counter-espionage. We knew exactly which aides at the embassy interested SIS, and when and how they would be approached by our opposite numbers. We had the names of all those who the British believed could be persuaded to defect. We were also fully aware of every detail of the work being done by [MI5] against the British Communist Party. We knew the whereabouts of their bugs, the identities of their agent provocateurs, who their agents were and what information they were providing. ... In hindsight, I can claim with absolute certainty that for most of the war we were able to work under ideal conditions in the British capital, simply because our risks were negligible. We operated with the extraordinary advantage of knowing in advance exactly how far we could go. Very few secret services in the world have been able to work under such fabulous conditions. (Modin 1995)

Even partially discounting the above recollection as bravado in retirement, knowing intimately the details of an adversary's capabilities to operate against one's own efforts must surely be regarded, like Modin claims, as 'ideal'.

No direct loss of life can be specifically traced to Blunt's treachery. However, he revealed the British intelligence community's greatest wartime achievements – Ultra and the Double-Cross system – to Stalin, who was to replace Nazi Germany as the primary threat to British security in the post war period. Blunt's undermining British counterintelligence permitted the KGB London residency to operate with near impunity. Despite his success as a spy, Blunt nearly broke under the strain of his double life, and his Soviet controllers agreed that he should unburden himself of it, not least because his access had dwindled and his stress was starting to become a liability for the others in the network. In 1964, Blunt confessed to British authorities in exchange for immunity from prosecution. However, in 1979 Prime Minister Margaret Thatcher publicly stripped then-Sir Anthony of his Knighthood. He died of a heart attack at home in London in 1983, best remembered not for his scholastic contribution to art history, but for his wartime betrayal of his country.

Guy Burgess, whose ideological commitment surpassed even Philby's, began his intelligence career in 1939 thanks to a secondment from the BBC to the Security Service to assist with wartime propaganda efforts (Lownie 2015). He also worked in SOE Section D alongside Philby. Burgess then found himself at the BBC during the early phases of the War, engaging in propaganda on behalf of Moscow. During the latter phase of the war Burgess provided the KGB with details of key summits between President Franklin Roosevelt and Prime Minister Winston Churchill, such as at Casablanca and Quebec, including the concept of operations for Overlord and for Husky, the Allied invasion of Sicily (Modin 1995).

While Burgess' postwar personal life was ever more erratic, thanks to appointment as private secretary to Hector McNeil, Minister of State for the Foreign Office, Burgess supplied Moscow with all diplomatic materials related to 1946 Paris Peace conference and again in the 1947 Council of Ministers meeting in Moscow. Burgess's efforts revealed British (and American)

negotiating positions and surely impacted the post war peace settlements in favor of Stalin. The following year he rejoined the Foreign Office and occupied a post in the Far Eastern Department (Lownie 2015). In 1949, Burgess went from passive provider of information to instigator of Soviet 'Active measures' to foment and exploit Anglo-American antagonism over China. In 1950 he provided KGB with British Army Intelligence corps appreciation of Soviet aid to Chinese and North Korean forces, again letting Stalin calibrate precisely how far to push (Modin 1995). The following year Burgess accompanied his friend Donald Maclean to Moscow, barely a step ahead of British authorities. After his defection, Burgess found that his adopted country was not as idyllic as he had imagined it. In 1963, he drank himself to a premature death in his new homeland. Burgess' efforts on behalf of the KGB caused lasting damage to Anglo-American national security, ensuring his spot within, but not atop, the most damaging spy ring in history (Lownie 2015).

Donald Maclean, a graduate of Trinity Hall, Cambridge, was also the only member of the Five to make his career in the Foreign Office instead of the intelligence or security establishment. This is not to say, however, that his treachery had lesser value or did less damage than his compatriots. In fact, Maclean's assignments in the Foreign Office were some of the most consequential during the latter part of the Second World War and into the early Cold War (Cecil 1988). After passing the KGB reams of diplomatic correspondence between London and Washington between 1940 and 1944, he was assigned as First Secretary at the British Embassy in Washington – a 'dream come true' for the KGB, which 'could hardly contain its glee' (Lownie 2015). In Washington, he was assigned as secretary for the closely guarded Anglo-American (and Canadian) Combined Policy Committee on atomic development, which reported directly to Roosevelt and Churchill. This position provided Maclean – and Moscow – with a front row seat for the political and broad stroke technological aspects of development of the atom bomb, known as the Manhattan Project (and Tube Alloys in Britain) (Andrew 1990).¹⁵ Moreover, based on Maclean's intelligence, Moscow could estimate how many atomic weapons that the US might be able to produce. Stalin's inside knowledge of America's nuclear stockpile – thanks to Maclean – likely emboldened his moves in Berlin in 1948 (Royal Air Force Museum, n.d., 1). Thanks also to his presence in Washington, Maclean was privy to American calculations about Truman's Containment doctrine, thus letting Stalin calibrate his hegemonic efforts right up to the edge, but without going too far.

If Stalin was ultimately able to restrain himself in Berlin, Maclean was unable in Egypt. After a drunken rampage in Cairo, (Maclean's posting after Washington), Maclean returned to work in London, assuming key duties as the head of the American Department, thereby ensuring Moscow's continued peek behind Anglo-American policy planning curtain (Cecil 1988). Although Maclean had already provided much to KGB, the beginning of the Korean War in 1950 provided yet another opportunity for Maclean to provide Moscow with an avenue to aid their fellow communists. Robert Cecil, Maclean's

¹⁵ Additional scientific material, such as the technical information for nuclear fission, was being provided to Moscow through Klaus Fuchs, Bruno Pontecorvo, David Greenglass, and Ted Hall. On this, see Andrew, Christopher (1990) *KGB*, Harper Collins.

Deputy on the American Desk, believed that Moscow would have assessed Maclean's documents 'of inestimable value in advising the Chinese and North Koreans on strategy and negotiating positions' (Andrew 1990). The following year, warned by Kim Philby that his days as a free man in Britain were numbered, Donald Maclean defected with his friend and co-conspirator Burgess to Moscow, where he remained until his death in 1983. Unlike Burgess, Maclean assimilated quite well, learning the language and consulting to the Soviet government on foreign affairs. But, perhaps tellingly, Maclean requested that his ashes be returned to England after his death (Royal Air Force Museum, 2).

Yuri Modin provided a nuanced appreciation of value, or damage, by comparing the product of Philby with that of Maclean. To borrow from the three identified levels of war, Philby was tactically the superior agent. Modin: 'If the criterion for judging an agent is the quantity and quality of the information he supplies, I can attest that what Philby produced was invariably flawless and immediately exploitable, concerning the activities of the other side, the locations of their agents and their attempts to mount sabotage operations.' However, the strategic and operational levels must belong to Maclean. Modin again:

On the other hand, if one considers that the aim of espionage is to furnish governments and heads of state with information that will assist them in their decisions, then the spy of the century has to be Donald Maclean. He gathered the political, economic and scientific intelligence that guided the strategy of our leaders for over ten years... During that period, the planet passed from a World War to a Cold War. What could be more crucial to the KGB at that time than to be fully informed of Anglo-American strategy vis-à-vis the Eastern Bloc? (Modin 1995).

Modin's assessment goes to the heart of the damage debate by considering sustained impact at the highest levels. While not all observers would agree with Modin's calculations, he reveals his own value framework by placing the agent and his information in broader strategic and historical context where it belongs.

Perhaps because he was not of minor aristocratic upbringing and he did not travel in the same social circles, John Cairncross is often excluded from membership in the Cambridge spy ring. This is unwarranted (Smith 2019). As Christopher Andrew observed, 'Though Cairncross is the last of the Five to be publicly identified, he successfully penetrated a greater variety of the corridors of power and intelligence than any of the other four' (Andrew 1990). Further, based on damage alone, he has 'earned' a place amongst his Cambridge peers (Andrews 2020).

In 1940-41, during service as Private Secretary to Lord Hankey (Chairman of the British Scientific Consultative Committee), Cairncross provided the first information to USSR about the Manhattan Project, years before Maclean, thus contributing to a rebalancing of global power, a key development in the proposed damage framework. In the words of David Leitch, 'His reports were instrumental in helping Russia to astonish the West by developing and exploding her own bomb' (Modin 1995). In 1942 he joined Bletchley Park, giving KGB yet another point of access to ULTRA, where he provided specific locations of German air force during battle of Kursk, earning a medal

commendation from Moscow. The Red Air Force destroyed the Luftwaffe planes on the ground in a pre-emptive strike that would shape the larger battle. In retrospect, ‘this series of three massive air raids was to be remembered as the greatest operation of the Red Air Force in the Great Patriotic War’ (Andrew 1990).

Although less dramatic than codebreaking and great air raids, a department that the Center had yet to penetrate was the Treasury, which Cairncross accomplished. The impact of Cairncross’ betrayal there was a further boon to the Soviets. Modin recalled:

Cairncross began supplying a steady stream of files on every aspect of the financing of the British Army, the Royal Navy and the RAF, along with specific data on his country’s war budget – notably the economic contingencies to be planned should war break out with the Soviet Union.... We now knew exactly how much money had been set aside to build tanks and airplanes, and how much was slated for nuclear research. All of this was of capital importance to our own military. (Modin 1995)

Subsequently Cairncross became a bean counter for NATO and was knowledgeable about each country’s military contribution. Cairncross’ betrayals, when taken together with his Cambridge comrades, reveal a tremendous amount of damage.

Applying the framework

In the end analysis, an assessment of damage to national security must be more than a litany of documents stolen, lives lost, sources and collection capabilities compromised, and money lost. There must be some consideration of the size of the wake behind the boat. Malcolm Gladwell phrases the question elegantly: ‘What did more damage – Philby’s treachery or the subsequent obsession among spy officials with preventing future Philbys?’ (Gladwell 2014). It is no exaggeration to say that the paranoia of molehunters destroyed the careers of many outstanding intelligence officers, likewise sowed needless doubt over a multitude of quality agents, and stymied otherwise operationally sound intelligence collection initiatives. For instance, James Angleton was convinced that many worthy agents, including Oleg Penkovsky, were actually double agents dangled by the KGB (Gioe 2014).

Similarly, on the British side, MI5’s Peter Wright claimed that Security Service Director General Roger Hollis was actually a Soviet agent. Wright’s ‘conspiracy theories arguably did as much damage to the Service as Blunt’s treachery’, judged their official historian (Andrew 2009). This concatenation of breach followed by paranoia drove out promising officers, dampened morale, inhibited judicious risk tasking, retarded agent recruitment, and cost the British and American intelligence communities potentially untold riches in foregone intelligence reporting, particularly on the Soviet Union. In response to Gladwell’s question, it seems clear that the lasting damage by the Five to the transatlantic intelligence partners was to lead those exemplified by James Angleton and Peter Wright, into a ‘wilderness of mirrors, searching in vain for the chimera of a still vaster but imaginary Soviet deception’ (Andrew 1990).

What looking to the past provides is a starting point to aid the intelligence reckoning by employing the proposed damage framework. While there is latent potential for contemporary massive intelligence breaches (a deluge frequently referred to using the misnomer 'leaks') to have grave consequences, the gravest of these, loss of innocent life, remains hypothetical, and can only be conclusively demonstrated by an impossible counterfactual scenario. Given that the breaches of Snowden, Schulte, Manning and Winner are still relatively recent, it is difficult to measure the damage done by this new breed, but as this article argues, long-term historical perspective offers a useful lens for new phenomena.

The implications of counterintelligence failures and mass leaks from trusted insiders are hard to understate. Due to the demonstrable change in terrorist communications resulting from his leaks, the potential exists for Snowden's or Schulte's actions in particular to hamper American counterterrorism efforts to the point where a catastrophic attack could be missed and inevitably the loss of innocent life would follow. Likewise, while the new breed irreversibly hindered lawful and legitimate intelligence collection initiatives, not limited to counterterrorism, but including counter-intelligence, counter-narcotics, counter-proliferation, and major criminal networks, these compromises have not fundamentally re-ordered the balance of power in the international system.¹⁶

It is possible that leakers have sidelined important US foreign policy initiatives, hurt employee morale throughout the intelligence community, that officers to conduct damage assessments will come off of other national security missions, and these accountings will likely take years to complete. Finally, the financial costs to replace certain collection capabilities will be in the billions of dollars, not to mention the financial losses to the US technology sector.

While it may be argued that Snowden's leaks were a critical impetus toward a national discussion about governmental transparency in the name of national security, this slight amelioration is unable to offset the damage already done, nor any part of the unrealized potential damage that remains theoretical to date. A more careful selection of documents to leak – as in the Winner case or the Daniel Ellsberg case decades ago – may have aided this argument, but the scope of documents released and the programs compromised that were unrelated to concerns about domestic civil liberties and personal privacy inveigh against damage mitigation on the grounds of public interest whistleblowing. As the Congressional report made clear, 'the vast majority of the documents he stole have nothing to do with programs impacting individual privacy interests – they instead pertain to military, defense and intelligence programs of great interest to America's adversaries' (U.S. House of Representatives Report 2016).

As the intelligence community holds its collective breath and races to repair the breaches, the scope of the damage perpetrated by the Cambridge Five is clearer with over a half century of hindsight. Moscow's 'Magnificent Five' can be credited with loss of life hundreds of times over and the compromise of many sources as well as intelligence collection methods and counter-

¹⁶ While many question the legitimacy of the US Government's interpretation of the provisions of the PATRIOT Act that Snowden found objectionable, the preponderance of legal challenges have been unsuccessful so far.

Base case (a): Cambridge Five Comparison case (b): Snowden	Qualitative-Comparative Damage Framework				Factors
	Comparison to Base		Weighted Comparison		
	(x)	(y)	(b)	(a)	
Factor measurement / magnitude (x)					
Extremely costly in comparison - 5	1	1	1	24	1. Lives lost (often a function of the timeliness of intelligence)
Very costly in comparison - 4	2	3	6	19	2. Sources & methods compromised (a function of the placement & access a leaker has)
Moderately costly in comparison - 3	4	2	8	17	3. Cost of replacing lost collection capabilities
Slightly costly in comparison - 2	5	3	15	10	4. Economic or reputational damage done to relevant institutions or corporations
Not costly in comparison - 1	2	5	10	15	5. Stunted employee morale
	4	4	16	9	6. Redirected personnel resources for damage assessments
Factor Significance (y)	N/A	N/A	N/A	N/A	7. Geostategic disadvantage
Extremely significant in comparison - 5	1	3	3	22	a. Shifts in balance of power
Very significant in comparison - 4	2	3	6	19	b. Loss of national narrative in foreign policy initiatives
Moderately significant in comparison - 3	1	5	5	20	c. Impaired intel liaison
Slightly significant in comparison - 2	3	2	6	19	d. loss of future intelligence reporting streams
Not significant in comparison - 1					
	Result =		76	174	

Figure 2. Application of the framework.

intelligence tradecraft. The Five so exposed the Anglo-American intelligence and security establishment that the balance of power in relation to NATO war planning and postwar peace negotiations was tilted toward the Soviets while simultaneously driving a wedge in the special relationship. ‘Undoubtedly, the damage inflicted by Philby, Burgess and Blunt can only be described as colossal, and on a much greater scale than has ever been published,’ judged intelligence historian Nigel West (West et al 1999). As Malcolm Gladwell and Christopher Andrew suggested, the legacy of paranoia and mistrust that the Five left in their wake had repercussions reverberating through the end of the Cold War.

While any conclusion regarding the comparative damage assessment involving relatively recent leaks must be a tentative one for several years to come, the proposed framework can aid damage analysis by academic researchers as well as counterintelligence professionals. It remains to be seen whether America’s intelligence relationships with its closest partners will be adversely affected. Although Germany curbed joint intelligence collection after the Snowden revelations (Smale 2015) indications are that the Five Eyes alliance will weather the storm. Other key indicators will be the resolution (if any) of the FBI and MI5 versus Silicon Valley ongoing crypto-war or if the NSA’s new statutory limitations on collection programs will force it to protect America with one hand tied behind its back.

Despite these complexities the framework put forward in this article offers a structured way to answer the fundamental comparative question. As mentioned earlier, Snowden’s leaks have never been linked to any lives lost, unlike the many hundreds attributed to the Cambridge Five. The lives lost as a result of the Five’s treason certainly were significant and directly impacted the future of Albania, per the discussion above, as well as dealt a blow to joint Cold War operations. There is also little in either case to consider ‘lives lost,’ considered as a factor, more or less significant. For these reasons the lowest Likert scale categories are deemed appropriate for both (x1) and (y1) in the framework depicted in Figure 2. Evaluating the second factor, the sources and methods compromised by the respective breaches, is less straightforward. Only members of the intelligence community are in positions to measure the cost that Snowden’s revelations had on sources and methods. Taking them at their word, terrorists and other individuals have altered their behavior as a result of Snowden’s actions – leading to a real loss of capability. Nevertheless, the GCHQ’s lamentation that capabilities which once took two weeks now takes six weeks to deliver hardly, except in the case of a ticking-bomb scenario,

amounts to an unrecoverable loss of sources and methods (Moore et. al., 2014). Measuring the comparative significance of sources and methods losses between the two case studies is problematic due to their difference in kind and quantities (particularly the vast quantities of SIGINT and COMINT agencies are able to access today). Nevertheless, against the backdrop of the Cold War, when compared to the hegemony the US still enjoys, one might conclude that sources and methods in the past—as a factor—were probably very significant compared to today. Snowden's leaks were therefore only slightly costly in their impact on sources and methods in comparison with that of the Cambridge Five and not more than moderately significant as a factor, given their respective historical contexts.

Measuring the comparative cost of replacing lost collection capabilities is, as noted above, less than straightforward. While Snowden's leaks and the activity of the Cambridge Five affected sources and methods from a number of countries, the US and UK have been, of course, most directly affected by their resultant replacement costs. Of course, the burden of cost depends upon a comparison between the types and severity of the sources lost in each of our cases, but also in the relative ability to pay for them. In the case of the Cambridge Five, more human (and therefore cheaper) sources were burned relative to Snowden's leaks, which betrayed sophisticated technologies. Such technologies require a sophisticated infrastructure of computer clusters, specialized hardware, trained cryptographers, software developers, and so on. Compared to the day-to-day budget required to train and run human agents, paramilitary Albanians, and other forces, such technological costs are very costly by comparison.

Yet this source type-related gap closes considerably when one considers the comparative resources available over time to bear such cost-burdens – thereby decreasing the significance of replacement cost as a damage assessment factor. Both countries have until recently kept details of their intelligence budget secret. Nevertheless, since approximately three of every four intelligence dollars goes to the Defense Department, the ratio of DoD's budget relative to gross domestic product (GDP) acts as a reliable proxy for the US intelligence budget. World Bank data shows that GDP increases over time has cut the DoD budget from around nine percent in 1960 to 3.8 percent in 2013, the year Snowden leaked his material. This has fallen still further since then and was a little over three percent in 2018 (World Bank Report, 2018). In the UK, where GCHQ is a civilian organization and does not fall under the Ministry of Defence (MoD), this measurement is less reliable. Nevertheless, using it shows that in 1960 defense spending was 6.3 percent of GDP while in 2013 it had fallen to two percent. By 2018 it had fallen again to a mere 1.6 percent (World Bank Report 2019). Given the overall growth of Western economies in the post-war period, it seems clear that while the technological nature of lost sources has, in the case of Snowden, placed a comparative cost burden on the part of the US and UK, their economies are in a far better position to bear such costs. As such, the significance of the cost-factor in the Snowden leaks is slight when compared to that of the Cambridge Five.

As discussed above, institutions and corporations lost substantial revenues—hundreds of billions of dollars in cloud computing alone—due to the reputational damage inflicted by Snowden's leaks (Kehl et al 2014). Because

the companies discovered to have relationships with both the NSA and GCHQ had a wide customer base among the general population, the magnitude of the reputational impacts were extremely significant. Nothing in the case of the Cambridge Five comes close to this. Similarly, as a factor, compared to the Cambridge Five case the economic or reputational impacts of national security information breaches remain significant. However, this significance is moderated by the observation that no mass exodus on the part of customers from Verizon, AT&T, and other companies affected by the Snowden leaks was observed. Companies have learned to weather public relations storms in a variety of ways, diminishing the long-run impact of the temporary loss of public trust. Most companies affected by Snowden's revelations employed a successful two-pronged public relations strategy wherein they denied having any knowledge of secret programs having code names such as 'PRISM', which was technically true since NSA code names were not given to companies, and shifting blame to the government by pointing out, correctly, that they only acted in accordance with what was required of them by law (Corera 2015).

The damage done to employee morale by the Cambridge Five, discussed above, is well-documented. The search for the 'Third Man,' and, after Philby's defection, the fourth- and fifth-men, paralyzed intelligence agencies on both sides of the Atlantic for years. Alleged outings of a 'Sixth Man' continue to the present day, with 2015 charges against former MI6 physicist Wilfred Mann and Cambridge dropout Cedric Belgrave just the latest in a long string of investigations (Jamieson 2015). As has been noted, the paranoia of CIA counterintelligence czar James Angleton knew no limits in the wake of Philby's defection. Angleton's subsequent mole-hunt stunted that agency's efficacy for a generation (Hoffman and Ostermann 2014). In the immediate aftermath of the Snowden leaks, NSA officials reported wide employee disillusionment at the agency, with the hit to morale especially acute because President Obama failed to visit Fort Meade to offer his support, unlike his predecessor during the so-called 'warrantless wiretapping' scandal. NSA clerks noted a surge in resume clearance requests, required of NSA employees seeking to list national security credentials during job searches (Nakashima 2013). Steven Levy of *Wired Magazine* interviewed NSA officials in 2014 and noted that depleted morale continued to plague the organization: 'Morale suffers when friends and neighbors think that NSA employees are sitting around reading grandma's email' (Levy 2014). Nevertheless, the effect on employee morale at NSA was acute but relatively temporary. In 2018, US officials speaking to the Washington Post reported that morale continued to be an issue at the agency but attributed this to low pay, a very unpopular reorganization, and continued leaks not related to Snowden's (Nakashima et al 2018). It is difficult not to conclude that had these exogenous (to Snowden) factors not been present and President Obama had vocally supported the NSA as his predecessor had done, the morale effects of the greatest breach in NSA's history would have been negligible. Such a statement cannot be said of the havoc wreaked on morale in the wake of the Cambridge Five.

Therefore, measured in comparative magnitude Snowden's impact on NSA morale was relatively slight. Nonetheless, the importance of morale today is arguably much higher than in the days of the Cambridge Five. NSA (and presumably GCHQ) job interviews target both an applicant's skills and her

cognitive processes because what is being sought is a certain kind of mind that will excel in the advanced world of computer hacking, cryptography, signals collection, and so on. The NSA is reportedly between five and ten years ahead of the private sector, and to keep this edge it must attract and retain the best and brightest employees (Szoldra 2016). In a highly-advanced economy, where a single successful NSA hacking operation might yield terabytes of an enemy's sensitive data, employee degradation due to negative morale threatens intelligence services in a way that simply didn't exist when the Cambridge Five were stuffing documents into their briefcases. Thus, morale as a factor can reasonably be considered extremely significant in the case of Snowden when compared to that of the Cambridge five.

The costs associated with redirecting personnel and resources for damage assessment is somewhat more straightforward given the technological differences between the Cambridge Five and Snowden cases. While the Cambridge Five had access to sensitive national security information spanning a remarkable variety of institutions and government agencies, including information acquired through liaison with the US, the amount of total information was relatively small by comparison to that compromised by Snowden. Still, damage assessments associated with the Cambridge Five were undertaken for decades since the mole-hunt continued long after the compromises had run their courses. And Philby's betrayal in particular wreaked outsized havoc on the CIA through Angleton's aforementioned paranoia. Nevertheless, modern data-storage capabilities simply dwarf the ability of even the most capable spy ring in history to compromise information over decades. Even with the help of those same technological capabilities, the task of cross-referencing every piece of information leaked in Snowden's 50 terabytes of stolen data, their dissemination paths, their potentially now compromised collection methods, and even their storage-medium locations, which must be undertaken by contemporary formal assessment teams, is daunting. It is therefore reasonable to conclude that the damage assessment costs associated with Snowden's leaks are comparatively very costly. Since the opportunity costs associated with redirecting the tasks of much sought after personnel, as described above, are so high, it might also be concluded that compared with the days of the Cambridge Five damage assessment costs as a factor is very significant. These evaluations are reflected in [Figure 2](#) above.

The final category in the framework involves determining the way in which four sub-factors contribute to an evaluation of the geostrategic disadvantages caused by insider threats to national security information. These sub-categories can be considered individually but interrelate in such a way that their amalgamation produces geostrategic disadvantages to insider threat victims, be they victims of externally tasked insider threats or internally motivated ones. In light of what has already been considered above, evaluating the first sub-category—shifts in the balance of power—is less problematic. Despite the magnitude of the Snowden leaks, nothing currently known about the nature of the material compromised even remotely challenges US hegemony in the contemporary international structure of power. Compared to the strategic importance of the Cambridge Five's betrayals, which included, among much else, information that aided Soviet nuclear strategy during critical periods of the Cold War, Snowden's leaks were simply not costly in comparison. The importance that

shifts in the balance of power, as a factor, has is less one-sided. Despite US hegemony, a weakening in the balance of power today might further close the relative power gap between its contemporary rival, China. But compared to significance that a tipping of the balance of power in favor of the Soviets might have had, in the bipolar world of US-Soviet co-dominance, this factor today probably does not exceed moderate significance.

Geostrategic disadvantage also depends upon a loss of national advantage in foreign policy initiatives. On 9 June 2013, the very day Edward Snowden went public as the NSA leaker in an interview in a Hong Kong hotel, the Obama administration was preparing the final diplomatic crescendo of a coordinated US campaign against China's cyber espionage—its monumental theft of industry research and development efforts. Within hours documents were published online detailing America's doctrine for offensive cyber operations, giving ammunition to Chinese negotiators and undermining the Obama administration's moral authority. Ultimately the planned confrontation by the US, according to officials, 'fizzled out' (Corera 2015). Additionally, a diplomatic row ensued when Snowden's leaks seemed to show that the US had collected data from Germany's Chancellor Angela Merkel for years. A subsequent revelation, this time with an American official as victim, revealed that German security services had done the same against then-US Secretary of State John Kerry's communications. Pragmatically, both countries quickly moved on, suggesting that the context within which breaches are conducted may be more significant to damage assessments than the breaches themselves (BBC, 2015). Such strains on foreign policy are miniscule in magnitude compared to the policy impacts of the Cambridge Five, whose work helped, among much else, vitiate the post-war West's most prized strategic objective: protecting information about its nuclear programs and policies. When compared to the undermining of apocalypse-preventing goals, the impact of Snowden's leaks on contemporary US-UK foreign policies is vanishingly small. Yet as with the previous factor, a comparison of the geo-strategic situation in which the US and UK find themselves today vis-à-vis during the Cold War probably means that, as a factor, national security information breaches remain of moderate significance.

There is little evidence to suggest that either Snowden or the Cambridge Five breaches made significant lasting impacts to intelligence liaison relationships, although the betrayal of the Five was more consequential and both were felt sharply in their respective moments, especially as the British had to endure several iterations of shame and outrage as the Five were unmasked over time. Still, the health of such partnerships is shaped by broader factors than the occurrence of breaches, which every side understands will happen from time to time. This cost of doing business is, in the case of Snowden, and always was, in the case of the Cambridge Five, balanced against the benefits both the US and UK attain from continuing their liaison in light of breaches. Moreover, technological progress has meant that the importance of liaison has arguably increased over time, specifically for the US and UK. Packet-switching networks, such as the internet, send information in separate chunks (called 'packets') by means of a global system of routers. Therefore, modern cyber espionage requires access to global network infrastructures that can most easily be accessed through international cooperation.

Finally, the loss of future intelligence reporting streams can significantly undermine a nation's geostrategic position because it robs policymakers of insights and gives global competitors a knowledge-advantage, to be used on the battlefield or at the negotiating table. Thus, unlike the third factor in the framework, the cost of intelligence reporting streams drying up is here measured in terms of the informational impacts to strategy. This, in turn, is a function of what is at stake in the strategic international order in which the information plays its part. Again, the hegemony enjoyed by the United States today is such that the strategic informational cost of Snowden's national security information breach is not more than moderate when compared to the information lost by the US and UK during critical moments of the Cold War. For the same structural reason, informational cost as a factor in assessing damage, is perhaps only slightly significant in the case of Snowden when compared to the Cambridge Five.

By enumerating the Likert-scale qualitative categories, the damage assessment framework offered (and represented in [Figure 2](#) above) offers an analytical tool to structure our thinking about the comparative costs of the Snowden leaks and the espionage of the Cambridge Five. This framework does not represent a nomologically deterministic algorithm by means of which convergence on an answer is preordained. As such, the numerical results produced by the framework are meant to guide broad conclusions rather than offer specificity in measurement.

Conclusion

After this review and analysis, we return to the question that instigated this article: Is Snowden's place at the pinnacle of the traitor's pantheon warranted? With the application of a more textured understanding of damage through insider threats, and with the benefit of historical perspective, the definitive answer is no (or perhaps 'not yet'). Even without such a verdict, however, the implications of trusted insiders with special system access privileges are profound, revealing the scope of the challenge for intelligence and security communities as well as their oversight bodies. Technology – in the early 21st century – favors the leaker from the inside and the hacker from the outside. Armed with a facilities access badge, a systems user account, and an inexpensive flash drive, an insider threat like Snowden, Manning, or Schulte could fit far more classified information on a keychain or wallet of compact discs than the Cambridge Five could have removed from the British secret state over a lifetime.

The capabilities of trusted insiders to exfiltrate classified data has shaken intelligence communities to the core, but the damage assessment framework offered here provides a way to calibrate and assess competing claims of damage to national security, helping policymakers, privacy advocates, technologists, academics, and intelligence mandarins understand, contextualize, and respond to this phenomenon. More broadly, this article advances our understanding of international affairs through the lens of compromises to national security and their international implications.

Notes on contributors

David V. Gioe is Associate Professor of History at the US Military Academy at West Point, where he also serves as History Fellow for the Army Cyber Institute. He is Visiting Senior Research Fellow in the Department of War Studies at King's College London, and Director of Studies for the Cambridge Security Initiative's International Security and Intelligence program. His areas of expertise are applied contemporary history, strategic and intelligence studies. Email: David.Gioe@Westpoint.edu

Joseph M. Hatfield is Associate Chair of the Cyber Science Department at the United States Naval Academy and is an active duty intelligence officer with over a decade of overseas operational experience. Hatfield's areas of expertise are Intelligence Studies, Cyber Operations, ethics and political theory. Email: hatfield@usna.edu

ORCID

David V. Gioe  <http://orcid.org/0000-0003-4310-999X>

References

- Albrecht, Jan Philipp (2015). 'Hands off our data!' *Knaur Taschenbuch* [online]. https://www.janalbrecht.eu/wp-content/uploads/2018/02/JP_Albrecht_hands-off_final_WEB.pdf
- Ahlberg, Christopher (2014) 'Al-Qaeda and Snowden: correlation, causation, and temporal analysis', *Recorded Future Blog*, 6 August. <https://www.recordedfuture.com/al-qaeda-encryption-technology-reaction/>
- Alford, Fred C (2002) 'Whistleblowers and the Narrative of Ethics', *Journal of Social Philosophy*, 4: 402–418 'Notably, this debate has included the Anglophone 'Five Eyes' Signals Intelligence alliance and has triggered research in member countries. For instance, see Friedman, Mark (2015) 'Edward Snowden: Hero or Traitor? Considering the Implications for Canadian National Security and Whistleblower Law', *Dalhousie Journal of Legal Studies*, 24
- Aid, Matthew (2014) 'Snowden revelations have sparked boom in data encryption in Germany' *Associated Press*, August 7. <http://www.matthewaid.com/post/94093523421/snowden-revelations-have-sparked-boom-in-data>
- Amble, John (2013) 'Everybody Spies' *War On The Rocks*, 9 July. <https://warontherocks.com/2013/07/everybody-spies/>
- Andrew, Christopher (2004) 'Intelligence, international relations and 'under-theorisation', *Intelligence and National Security*, 19:2, 170–84
- Andrew, Christopher (2009) *Defend the realm* (New York: Random House)
- Andrew, Christopher (1990) *KGB* (New York: Harper Collins)
- Andrew, Christopher, and Vasili Mitrokhin (1999) *Sword and the shield* (New York: Basic Books)
- Andrews, Geoff (2020) *Agent molière: the life of john cairncross, the fifth man of the Cambridge spy circle* (London, I.B. Tauris)
- Bamford, James (2014) 'Edward Snowden: the untold story', *Wired*, 13 June. <https://www.wired.com/2014/08/edward-snowden/>
- Bang, Martin (2016) 'Pitfalls in military quantitative intelligence analysis: incident reporting in a low intensity conflict', *Intelligence and National Security*, 31:1, 49–73
- BBC New (2015) 'Snowden NSA: Germany drops Merkel phone-tapping probe.' 12 June. <https://www.bbc.com/news/world-europe-33106044>
- Borger, Julian (2013) 'Edward Snowden's choice of Hong Kong as haven is a high-stakes gamble', *The Guardian*, 9 June. <http://www.theguardian.com/world/2013/jun/09/edward-snowden-hong-kong-gamble>

- Boyle, Andrew (1979) *The climate of treason: Five who spied for Russia* (London: Hutchinson and Co)
- Capra, Tony (2014) 'Snowden leaks could cost military billions: pentagon', *NBC News*, March 6. <http://www.nbcnews.com/news/investigations/snowden-leaks-could-cost-military-billions-pentagon-n46426>. Notably, Dempsey placed relatively long time horizon of the damage mitigation efforts ahead of the financial costs, perhaps suggesting in his view that they belong in that order
- Carter, Miranda (2001) *Anthony blunt: His lives* (New York: Farrar, Strauss, Giroux)
- Cecil, Robert (1988) *A divided life: a biography of Donald Maclean* (London: The Bodley Head)
- Cole, Matthew, and Mike, Brunner (2014) 'Edward Snowden: A Timeline', *NBC News*, 26 May. <http://www.nbcnews.com/feature/edward-snowden-interview/edward-snowden-timeline-n114871>
- Corera, Gordon (2015) *Cyberspies: the secret history of surveillance, hacking, and digital espionage* (New York: Pegasus Books)
- Delmas, Catharine (2015) 'The ethics of government whistleblowing', *Social Theory & Practice*, 32:1, 77–105
- Dulles, Allen (2006) *The craft of intelligence* (Guilford: Lyons Press)
- Financial Times (2013) 'The Security Threat Posed by Snowden', 9 October <http://www.ft.com/intl/cms/s/0/9b4b5afe-30dc-11e3-b991-00144feab7de.html#axzz3Q1sLUCDb>. GCHQ fury at the NSA is understandable and justified, but likely short-lived in light of the interconnected nature of the two organizations
- Flyvbjerg, Bent (2001) *Making social science matter* (Cambridge: Cambridge University Press)
- Flyvbjerg, Bent, Todd Landman, and Sanford Schram (eds.) (2012) *Real social science: applied phronesis* (Cambridge: Cambridge University Press)
- Gaspard, Jules (2017) 'Intelligence without essence: rejecting the classical theory of definition', *International Journal of Intelligence and Counterintelligence*, 30:3, 557–82
- Gioe, David V (2014) 'Tinker, tailor, leaker, spy: the future costs of mass leaks', *The National Interest*, January/February
- Gladwell, Malcolm (2014) 'Trust no one: Kim Philby and the hazards of mistrust', *The New Yorker*, 28 July. <https://www.newyorker.com/magazine/2014/07/28/philby>
- Goldman, Adam (2018) 'New Charges in Huge CIA Breach known as Vault 7', *New York Times*, 18 June. <https://www.nytimes.com/2018/06/18/us/politics/charges-cia-breach-vault-7.html>
- Gros, Valentin, Marieke de Goede, and Beste İşleyen (2017) 'The snowden files made public: a material politics of contesting surveillance', *International Political Sociology*, 11:1, 73–89
- Hatfield, Joseph M (2018) 'Social engineering in cybersecurity: the evolution of a concept', *Computers & Security*, 73, 102–113.
- Hatfield, Joseph M (2017) 'An ethical defense of treason by means of espionage', *Intelligence and National Security*, 32:2, 195–207
- Herbig, Katherine L (2017) 'The Expanding Spectrum of Espionage by Americans, 1947–2015', *PERSEC Technical Report 17-10*, Department of Defense. https://www.dhra.mil/Portals/52/Documents/perserec/reports/TR-17-10_The_Expanding_Spectrum_of_Espionage_by_Americans_1947_2015.pdf
- Heuer, Richards J (2009) 'The Evolution of Structured Analytic Techniques', *Presentation to the national academy of science, national research council committee on behavioral and social science research to improve intelligence analysis for national security* (Washington, DC, December 8, 2009)
- Hoffman, Bruce, and Christian Ostermann (2014) *Moles, defectors and deceptions: James angleton and his influence on US counterintelligence* (Washington, DC: Woodrow Wilson International Center for Scholars)
- King, Gary, Robert O Keohane, and Sidney Verba (1994) *Designing social inquiry: Scientific inference in qualitative research* (Princeton: Princeton University Press)
- Jamieson, Sophie (2015) 'Sixth member of the Cambridge spy ring revealed', *The Telegraph*, 6 September. <https://www.telegraph.co.uk/news/uknews/defence/11847477/Sixth-member-of-Cambridge-Spy-Ring-revealed.html>

- Jones, Sam (2015) 'Cedric Belfrage – The 'Sixth Man' Soviet spy who hid in plain sight', *Financial Times*, 20 August. <https://www.ft.com/content/c3c3bf66-4751-11e5-af2f-4d6e0e5eda22>
- Kehl, Danielle, Kevin Bankston, Robyn Greene, and Robert Morgus (2014) 'Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom, and Cyber Security', New America Foundation Open Technology Institute Policy Paper, July
- Levy, Steven (2014) 'I Spent Two Hours Talking with the NSA's Bigwigs. Here's What Has Them Mad', *Wired*, 13 January. <https://www.wired.com/2014/01/nsa-surveillance/>
- Lownie, Andrew (2018) *Stalin's Englishman: guy burgess, the cold war, and the Cambridge spy ring* (New York: St. Martin's Press)
- Maass, Harold (2013) 'Did Edward Snowden's Leak Make Americans Less Safe?', *The Week*, 11 June. <http://theweek.com/articles/463354/did-edward-snowdens-leak-make-americans-less-safe>
- Macintyre, Ben (2018) *The spy and the traitor* (New York: Crown Publishers)
- Macintyre, Ben (2014) *A spy among friends* (New York: Crown Publishers)
- Meyers, Lawrence S, Anthony Guarino, and Glenn Gamst (2013) *Applied multivariate research: Design and interpretation* (London: Sage Publications)
- Modin, Yuri (1995) *My five cambridge friends* (New York: Macmillan)
- Moore, Charles, and Tom Whitehead (2014) 'Edward Snowden leaks mean GCHQ takes three times as long to track terrorists', *The Telegraph*, 11 October
- Morell, Michael (2013) Interview with CBS '60 Minutes', 30 October. <http://www.cbsnews.com/news/the-deputy-director-mike-morell/>
- Nakashima, Ellen (2013) 'NSA Morale Down After Edward Snowden Revelations, Former U.S. Officials Say', *Washington Post*, 7 December. https://www.washingtonpost.com/world/national-security/nsa-morale-down-after-edward-snowden-revelations-former-us-officials-say/2013/12/07/24975c14-5c65-11e3-95c2-13623eb2b0e1_story.html
- Nakashima, Ellen, and Aaron, Gregg (2018) 'NSA's top Talent is Leaving Because of Low Pay, Slumping Morale and Unpopular Reorganization', *Washington Post*, 2 January. https://www.washingtonpost.com/world/national-security/the-nas-top-talent-is-leaving-because-of-low-pay-and-battered-morale/2018/01/02/ff19f0c6-ec04-11e7-9f92-10a2203f6c8d_story.html?noredirect=on
- Peterson, Andrea (2013) 'The NSA has its own team of elite hackers', *The Washington Post*, 13 August. <http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers/>
- Pherson, Randolph H, and Richards J Heuer (2021) *Structured analytical techniques for intelligence analysis* (Thousand Oaks, California: CQ Press)
- Philby, Rufina (1999) *The private life of kim philby* (London, St. Ermin's Press)
- Philipps, Dave (2018) 'Reality winner, former NSA translator, gets more than 5 years in leak of Russian Hacking Report', *New York Times*, 23 August
- Philipps, Roland (2018) *A spy named orphan: the enigma of Donald Maclean* (New York, W. W. Norton Co)
- Romano, Andrew (2014) 'New NSA director rips critics, calls for 'less simplistic' national conversation about surveillance', *Yahoo News*, 14 November. <https://news.yahoo.com/new-nsa-director-rips-critics-calls-for-a-less-simplistic-national-conversation-about-surveillance-005140623.html>
- Royal Air Force Museum, National Cold War Exhibition (n.d., 1) 'The Cambridge Four', <http://www.nationalcoldwarexhibition.org/schools-colleges/national-curriculum/espionage/the-cambridge-four.aspx>
- Royal Air Force Museum, National Cold War Exhibition (n.d., 2) 'Donald Maclean biography', <http://www.nationalcoldwarexhibition.org/the-cold-war/biographies/donald-maclean/>
- Sanger, David E (2014) 'New N.S.A. Chief Calls Damage From Snowden Leaks Manageable', *New York Times*, 29 June. http://www.nytimes.com/2014/06/30/us/sky-isnt-falling-after-snowden-nsa-chief-says.html?_r=0
- Schmitt, Eric and Michael S. Schmidt (2013) 'Qaeda Plot Leak Has Undermined U.S. Intelligence' *New York Times*, 29 September

- Smale, Alison (2015) 'Germany Limits Cooperation with U.S. Over Data Gathering', *New York Times*, 7 May
- Smith, Chris (2019) *The Last Cambridge Spy: John Cairncross, Bletchley codebreaker and soviet double agent* (Stroud, Gloucestershire, The History Press)
- Smith, Michael Douglas (2017) 'A good intelligence analyst', *International Journal of Intelligence and Counterintelligence*, 30:1, 181–5
- Snowden, Edward (2014) 'Here's how we take back the internet', *TED Talks*, March 201. http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet/transcript?language=en
- Szoldra, Paul (2016) 'Here's what it's like to interview for the NSA, from people who have done it.' *Business Insider*, 6 May. <https://www.businessinsider.com/nsa-job-interview-2016-5>
- U.S. House of Representatives (2016) 'Review of the unauthorized disclosures of Former National Security Contractor Edward Snowden', U.S. House of Representatives, 15 September. https://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_declassified.pdf.
- Van Cleave, Michelle (2015) 'What it takes: in defense of the NSA', *World Affairs*, 176:3 <https://fortunascorner.com/2013/11/05/what-it-takes-in-defense-of-the-nsa/>
- Weiner, Timothy (2007) *Legacy of ashes: the history of the CIA* (New York: Doubleday Books)
- West, Nigel, and Oleg Tsarov (1999) *The crown jewels: the British secrets at the heart of the KGB archives* (New Haven: Yale University Press)
- Whitehead, Tom, Christopher, Hope, and Steven, Swinford (2013) 'Sir David Omand: Snowden Leak is 'most catastrophic loss to British intelligence ever'', *The Telegraph*, 13 October. <http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/10371541/Sir-David-Omand-Snowden-leak-is-most-catastrophic-loss-to-British-intelligence-ever.html>
- Wintour, Patrick (2013) 'NSA Leaks: UK's enemies are 'rubbing their hands with glee' says MI6 Chief', *The Guardian*, 7 November 2013. <http://www.theguardian.com/world/2013/nov/07/nsa-leaks-enemies-rubbing-hands-glee-mi6>
- World Bank (2018) Stockholm International Peace Research Institute (SIPRI), Yearbook: Armaments, Disarmament and International Security. <https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS?locations=US>, accessed 1 September 2019
- Zetter, Kim (2010, 9 September) 'Massive Cache of Iraq War Docs to the Published by WikiLeaks', *Wired*